# The Critical Moment of Awareness

October 2009

ON CYBER PATROL
As covered or mandate
SARGE! I JUST HAD MY COMPUTER STOLEN!
AT LEAST IT'S ENCRYPTED, RIGHT?
Copyright U.S. Army. All rights reserved.
EXCEPT MY CAC WAS IN IT.
WHAT ABOUT YOUR PIN?
ON A NOTE STUCK TO THE COMPUTER
AND THEY ASK ME WHY I DON'T SLEEP AT NIGHT!
AC 1055

October is Cyber Awareness Month. This is an excellent effort to spread the word about cyber safety and reinforce the policies, procedures and best business practices that support sound information assurance (IA). Given the consequences of compromised military networks or the loss of Personally Identifying Information (PII), any program that helps get the message across is worth the time and effort .

But, what happens next month? There are many efforts, programs, initiatives, tasks and other duties competing for our awareness. Will cyber security and IA get lost in the noise as of 1 November? The people at the core of the Army's IA program would like it if every month was Cyber Awareness Month. It would make their jobs a lot easier and our networks a lot safer. Unfortunately, it's not in the budget. However, there is a cost-effective alternative: cyber awareness moments.

Moments are very brief, ranging from a split second to the rare, but memorable, like that "Hail Mary" pass into the end zone as time expires. It is within these tiny time spans – those key decision points – that IA is usually compromised. For example, the moment that someone clicks on an embedded web link in a phishing email, the moment a person decides to bypass data-at-rest (DAR) procedures, and the moment someone decides it would be a good idea to write his or her Common Access Card (CAC) Personal Identification Number (PIN) on a sticky note and leave it attached to his or her computer. These are examples of personal moments. Sometimes these moments can occur in a group setting like when people make the final decision to think about certification and accreditation of a new system "later," or when some enterprising soldiers decide on the spur of the moment to set up an unsecured network in theater so that they can play online games.

Now, if cyber awareness kicked in at those previously described moments, the chances of serious trouble due to hacked networks and stolen PII would be significantly reduced. This would be very efficient, given that there are most likely only five of these moments a day. Let's say the average moment is ten seconds long. That would be a mere 50 seconds a day devoted to having to be smart about IA. Such a small commitment of time would leave everyone plenty of time to be aware of other important things. So pay attention in October to the Cyber Awareness messages and then be very alert to those five daily IA decision point moments, less than a minute a day. It's not too much to ask for protecting missions and lives through good information assurance practices.